~~generating an available balance for the Counterparty based upon the at least one user-supplied risk parameter, payments made by the account holder, and payments received by the account holder;~~

~~reading the first instruction from the payment queue of the payment bank system; and~~

~~determining whether to selectively reject payment authorized by the first instruction based upon the available balance.~~

a' Sub B' cont-

~~60. The computer-implemented method of claim 59, wherein payment authorized by the first instruction is rejected in the event that the amount of payment authorized by the first instruction exceeds the available balance.~~

~~61. The computer-implemented method of claim 59, wherein the first instruction is returned to the payment queue for later re-evaluation in the event that the amount of payment authorized by the first instruction exceeds the available balance.~~

~~62. The computer-implemented method of claim 59, wherein the available balance is computed over a given time period based upon payments made by the account holder in the given time period and payments received by the account holder in the given time period.~~

~~63. The computer-implemented method of claim 62, further comprising the steps of:~~

~~receiving user-supplied updates to the at least one user-supplied risk parameter; and~~

~~updating the available balance to reflect such user-supplied updates.~~

~~64. The computer-implemented method of claim 63, further comprising the steps of: generating the user-supplied updates on a user system and communicating the user-supplied updates to the risk filter routine.~~

~~65. The computer-implemented method of claim 62, further comprising the steps of:~~

~~receiving updates to payments made by the account holder in the given time period; and~~

~~receiving updates to payments received by the account holder in the given time period; and~~

~~updating the available balance to reflect such updates.~~

~~66. The computer-implemented method of claim 65, wherein updates to payments made by the account holder and updates to payments received by the account holder are received through data interchange with existing payments confirmation services.~~

67. The computer-implemented method of claim 62, further comprising the step of receiving user-supplied updates to the at least one user-supplied risk parameter for use in the risk filter routine.

68. The computer-implemented method of claim 67, further comprising the steps of: generating the user-supplied updates on a user system and communicating the user-supplied updates to the risk filter routine.

a'. cont

69. The computer-implemented method of claim 57, wherein the risk routine is executed by a module integrated into the payment bank system.

70. The computer-implemented method of claim 57, wherein the risk filter routine is executed by a module that communicates to the payment bank system via an application-to application interface which translates data formats between the module and the payment bank system.

71. The computer-implemented method of claim 69, wherein the at least one user-supplied risk parameter is generated on a user system and communicated to a central server, which stores the at least one user-supplied risk parameter in a data server and forwards the at least one user-supplied risk parameter to the module integrated into the payment bank system that executes the risk filter routine.

72. The computer-implemented method of claim 57, wherein the at least one user-supplied risk parameter comprises a clean payment limit.

73. The computer-implemented method of claim 57, wherein the at least one user-supplied risk parameter is associated with each payment-based transaction wherein payment is made from the account holder to the Counterparty.

74. The computer-implemented method of claim 73, wherein the at least one user-supplied risk parameter is selected from the group consisting of:

(i) currency associated with each payment-based transaction,

(ii) payment type associated with each payment-based transaction, and

(iii) a Clean Payment Limit associated with each payment-based transaction.

75. The computer-implemented method of claim 73, wherein the at least one user-supplied risk parameter is associated with a first identifier that identifies the account holder and a second identifier that identifies the Counterparty on the payment transaction.

76. The computer-implemented method of claim 75, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

77. The computer-implemented method of claim 76, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party.

78. The computer-implemented method of claim 77, wherein said third party executes a third party host application that generates the at least one user-supplied risk parameter and communicates the at least one user-supplied risk parameter and associated information to a user system, which forwards the at least one user-supplied information to the risk filter routine.

a'. Cont.

79. The computer-implemented method of claim 78, wherein only the user system can forward the at least one user-supplied risk parameter communicated by the third party host application to the risk filter routine.

80. The computer-implemented method of claim 75, wherein the first and second identifiers are Bank Identifier Codes or an aggregation of such codes.

81. The computer-implemented method of claim 75, wherein the Counterparty comprises a beneficiary of the payment-based transaction.

82. The computer-implemented method of claim 57, wherein said risk filter routine cooperates with other payment processing operated by said payment bank to determine whether to selectively reject payment authorized by the first instruction.

83. The computer-implemented method of claim 57, wherein the risk filter routine cooperates with a domestic payment system operated by said payment bank, such that the first instruction is filtered by said risk filter routine for compliance with a risk profile generated from the at least one user-supplied risk parameter.

84. The computer-implemented method of claim 57, further comprising the step of : for each given first instruction, when processing by the risk filter routine rejects payment authorized by the given first instruction, adding the given first instruction to a cache of first instructions.

85. The computer-implemented method of claim 57, further comprising the step of communicating notification of rejection or success of at least one payment authorized by the first instructions stored in a cache.

86. The computer-implemented method of claim 85, wherein said notification is communicated via messaging services operably coupling the user system, a central system, and the payment bank system.

87. The computer-implemented method of claim 86, wherein a third party application is operably coupled to the payment bank system, and wherein said notification is forwarded to said third party application by said payment bank system.

88. The computer-implemented method of claim 85, wherein said notification is generated in the event that the Counterparty fails to make expected payments for a pre-determined period of elapsed time.

89. The computer-implemented method of claim 57, further comprising the steps of:

receiving a user-supplied second instruction that identifies an account holder and Counterparty; and

in response to receipt of the user-supplied second instruction, suspending all payments from the account holder to the Counterparty as identified by the second instruction.

a' cont.

90. The computer-implemented method of claim 89, wherein the user-supplied second instruction is generated on a user system and communicated to a central server, which stores the user-supplied second instruction in a data server and forwards the user-supplied second instruction to a modùle integrated into the payment bank system that executes the risk filter routine.

91. The computer-implemented method of claim 90, wherein a third party executes a third party host application that generates the user-supplied second instruction and communicates the user-supplied second instruction to a user system, which forwards the user-supplied second instruction to the module integrated into the payment bank system via the central server.

92. The computer-implemented method of claim 89, further comprising the step of: communicating notification confirming receipt and implementation of the user-supplied second instruction to the payment bank, core server, user and third party, if any.

93. The computer-implemented method of any of claim 89, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

94. The computer-implemented method of claim 93, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party as payment intermediary.

95. The computer-implemented method of claim 94, wherein said third party executes a third party host application that generates user-supplied instructions and communicates the user-supplied instructions to a user system, which forwards the at least one user-supplied instruction to the risk filter routine.

96. The computer-implemented method of any of claim 89, wherein the Counterparty comprises a payment beneficiary of the payment-based transaction.

A1 Cont.

97. The computer-implemented method of claim 57, further comprising the step of: using digital certification to establish access authority and usage constraints of the risk filter routine.

98. The computer-implemented method of claim 57, wherein data transmissions are encrypted for security purposes.

99. The computer-implemented method of claim 57, wherein users and the payment bank can also generate and receive payments-related notifications, inquiries, messages and reports.

100. The computer-implemented method of claim 57, wherein users can request and receive multi-currency reports from a plurality of Payment Banks acting on their behalf.

101. The computer-implemented method of claim 57, wherein human-accessibility is provided by browser interfaces and data-accessibility is provided by electronic data interchange formats.

102. The computer-implemented method of claim 57, wherein said account holder and Counterparty comprise multiple entities that are deemed to share correlation in payment risk assessment, wherein the multiple entities are identified by an aggregate identifier.

103. The computer-implemented method of claim 57, further comprising the steps of: recording various type of information, including identification of Users, identification of Third Parties, identification of Payment Banks, identification of Counterparties, identification of Currencies, specification of the Clean Payment Limit, and Payment Type identification.

104. The computer-implemented method of claim 57, wherein selective rejection of payment authorized by the first instruction reduces payment risk arising from default by the Counterparty and any liquidity risk and system risk arising therefrom in like amount.

105. A system for reducing risk in payment-based transactions comprising:

a payment bank subsystem, operated by a payment bank, that processes a payment-based transaction wherein payment is made from an account holder to a Counterparty, wherein the payment bank subsystem includes a queue storing a first instruction authorizing payment from the account holder to the Counterparty during processing of the transaction; and

a module, integrated with the payment bank subsystem, that stores at least one user-supplied risk parameter associated with the account holder, and includes a risk filter routine that operates during processing of the transaction to determine whether to selectively reject payment authorized by the first instruction stored in the queue based upon the at least one user-supplied risk parameter associated with the Counterparty.

106. The system of claim 105, wherein the risk filter routine:

generates an available balance for the Counterparty based upon the at least one user-supplied risk parameter, payments made by the account holder, and payments received by the account holder;

accesses a first instruction stored in the queue; and

determines whether to selectively reject payment authorized by the first instruction based upon the available balance.

a'. cont.

107. The system of claim 106, wherein the risk filter routine rejects payment authorized by the first instruction in the event that the amount of payment authorized by the first instruction exceeds the available balance.

108. The system of claim 106, wherein the risk filter routine returns the first instruction to the payment queue for later re-evaluation.

109. The system of claim 106, wherein the risk filter routine computes the available balance over a given time period based upon payments made by the account holder in the given time period and payments received by the account holder in the given time period.

110. The system of claim 109, wherein the risk filter routine receives user-supplied updates to the at least one user-supplied risk parameter, and updates the available balance to reflect such user-supplied updates.

111. The system of claim 109, wherein the risk filter routine receives updates to payments made by the account holder in the given time period and updates to payments received by the account holder in the given time period, and re-computes the available balance to reflect such updates.

112. The system of claim 111, further comprising a payment confirmation service, and wherein the risk filter routine receives updates to payments made by the account holder and updates to payments received by the account holder through data interchange with the payments confirmation service.

113. The system of claim 105, wherein the module communicates to the payment bank subsystem via an application-to application interface which translates data formats between the module and the payment bank subsystem.

114. The system of claim 105, wherein the at least one user-supplied risk parameter comprises a clean payment limit.

115. The system of claim 105, wherein the at least one user-supplied risk parameter is associated with each payment-based transaction wherein payment is made from the account holder to a Counterparty.

116. The system of claim 105, wherein the at least one user-supplied risk parameter is selected from the group consisting of:

(i) currency associated with each payment-based transaction,

(ii) payment type associated with each payment-based transaction, and

(iii) a Clean Payment Limit associated with each payment-based transaction;

a' Cont.

117. The system of claim 115, wherein the at least one user-supplied risk parameter is associated with a first identifier that identifies the account holder and a second identifier that identifies the Counterparty as payment beneficiary or intermediary on the payment transaction.

118. The system of claim 117, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

119. The system of claim 118, wherein the system includes a user subsystem executing a user host application that generates the at least one user-supplied risk parameter on a user subsystem and communicates the at least one user-supplied risk parameter to the module for use in the risk filter routine.

120. The system of claim 119, wherein the user subsystem generates user-supplied updates to the at least one user-supplied risk parameter and communicates the user-supplied updates to the module for use in the risk filter routine.

121. The system of claim 118, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party.

122. The system of claim 121, further comprising a third party host application that enables the third party to generate the at least one user-supplied risk parameter and communicate the at least one user-supplied risk parameter and associated information to a user subsystem, which forwards the at least one user-supplied information to the module for use in the risk filter routine.

123. The system of claim 122, wherein the third party host application enables the third party to generate updates to the least one user-supplied risk parameter and communicate the updates and associated information to a user subsystem, which forwards the updates and associated information to the module for use in the risk filter routine.

124. The system of claim 122, wherein only the user subsystem can forward the at least one user-supplied risk parameter communicated by the third party host application to the module for use in the risk filter routine.

125. The system of any of claims 118 to 124, wherein user-supplied risk parameter and updates thereto are communicated from the user subsystem to a central server, which stores the

at least one user-supplied risk parameter and updates thereto in a data server and forwards the user-supplied risk parameter and updates thereto to the module for use in the risk filter routine.

126. The system of claim 117, wherein the first and second identifiers are Bank Identifier Codes.

127. The system of claim 117, wherein the Counterparty comprises a payment beneficiary of the payment-based transaction.

a'
cont.

128. The system of claim 105, wherein said risk filter routine cooperates with other payment processing operated by said payment bank to determine whether to selectively reject payment authorized by the first instruction.

129. The system of claim 105, wherein the risk filter routine cooperates with a domestic payment system operated by said payment bank, such that the first instruction is filtered by said risk filter routine for compliance with a risk profile generated from the at least one user-supplied risk parameter.

130. The system of claim 105, wherein the risk filter routine, when processing a given first instruction results in a determination to selectively reject payment authorized by the given first instruction, and, whether selectively rejected or not, adds the given first instruction to a cache of first instructions.

131. The system of claim 130, wherein the risk filter routine triggers communication of a notification of rejection of at least one payment authorized by the first instructions stored in the cache to a user subsystem of the Payment Bank.

132. The system of claim 131, wherein said notification is communicated via messaging services operably coupling the user subsystem, a central subsystem, and the payment bank subsystem.

133. The system of claim 132, further comprising a third party application operably coupled to the user subsystem, wherein said notification is forwarded to said third party application by said user subsystem.

134. The system of claim 131, wherein said notification is generated in the event that the Counterparty fails to make expected payments for a pre-determined period of elapsed time.

135. The system of claim 105, wherein the risk filter routine:

receives a user-supplied second instruction that identifies an account holder and Counterparty; and in response to receipt of the user-supplied second instruction, suspends all payments from the account holder to the Counterparty as identified by the second instruction.

136. The system of claim 135, wherein the user-supplied second instruction is generated on a user subsystem and communicated to a central server, which stores the user-supplied second instruction in a data server and forwards the user-supplied second instruction to a module integrated into the payment bank subsystem that executes the risk filter routine.

a' cont.

137. The system of claim 136, wherein a third party executes a third party host application that generates the user-supplied second instruction and communicates the user-supplied second instruction to a user subsystem, which forwards the user-supplied second instruction to the module integrated into the payment bank subsystem via the central server.

138. The system of claim 136, wherein the risk filter routine triggers communication of notification confirming receipt of the user-supplied second instruction to the payment bank subsystem, core server, user subsystem and third party subsystem, if any.

139. The computer-implemented method of any of claim 135, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

140. The system of claim 139, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party.

141. The system of claim 140, wherein said third party executes a third party host application that generates user-supplied instructions and communicates the user-supplied instructions to a user subsystem, which forwards the at least one user-supplied information to the risk filter routine.

142. The system of any of claim 135, wherein the Counterparty comprises a beneficiary of the payment-based transaction.

143. The system of claim 105, wherein digital certification is used to establish access authority and usage constraints of the risk filter routine.

144. The system of claim 105, wherein data transmissions are encrypted for security purposes.

145. The system of claim 105, wherein users and the payment bank can also generate and receive payments-related notifications, inquiries, messages and reports.

146. The system of claim 105, wherein users can request and receive multi-currency reports from a plurality of Payment Banks acting on their behalf.

147. The system of claim 105, wherein human-accessibility is provided by browser interfaces and data-accessibility is provided by electronic data interchange formats.

148. The system of claim 105, wherein said account holder or Counterparty may comprise multiple entities that are deemed to share correlation in payment risk assessment, wherein the multiple entities are identified by an aggregate identifier.

149. The system of claim 105, further comprising a central core that records various type of information, including identification of Users, identification of Third Parties, identification of Payment Banks, identification of Counterparties, identification of Currencies, specification of the Clean Payment Limit, and Payment Type identification.

a'
Cont.

150. The system of claim 105, wherein selective rejection of payment authorized by the first instruction minimizes payment risk arising from default by the Counterparty and any liquidity risk and system risk arising therefrom.

151. The system of claim 144, wherein the data transmissions occur over a VPN that uses the Internet and other internet protocol telecommunication networks.

152. The system of claim 105, wherein the risk filter routine controls the flow of payment messages from the payment queue to a domestic payment system for clearance.

153. The system of claim 105, wherein the first instruction comprises a S.W.I.F.T. payment transaction.

154. The system of claim 112, wherein updates to the payments made by the Counterparty and updates to payments received by the Counterparty comprise S.W.I.F.T. messages.

155. The system of claim 105, wherein the risk filter routine interoperates with a plurality of payment channels for any given currency.

156. The computer-implemented method of claim 98, wherein the data transmissions occur over a virtual private network that uses the Internet and other internet protocol telecommunications networks.

157. The computer-implemented method of claim 57, wherein the risk filter routine controls the flow of payment messages from the payment queue to a domestic payment system for clearance.

158. The computer-implemented method of claim 57, wherein the first instruction comprises a S.W.I.F.T. payment transaction.

a' Cont
B'

159. The computer-implemented method of claim 66, wherein updates to the payments made by the Counterparty and updates to payments received by the Counterparty comprise S.W.I.F.T. messages.

160. The computer-implemented method of claim 57, wherein the risk filter routine interoperates with a plurality of payment channels for any given currency.

REQUIREMENT UNDER 37 C.F.R. §1.121

As required under 37 C.F.R. §1.121, a clean set of the pending Claims, as amended by the present Amendment, is as follows:

1. A system for reducing payments risk, liquidity risk and systemic risk associated with payments-based transactions, said system comprising:

a communications network formed by the interlinking of a plurality of internet protocol (IP) networks;

a plurality of User Host Applications supported over said communications network for use by plurality of Users active in payments-based transactions;

a plurality of Third Party Host Applications supported over said communications network for use by plurality of Third Parties active in payments-based transactions; and

a plurality of Payment Bank Host Applications supported over said communications network for use by a plurality of Payment Banks operating a plurality of domestic payment systems, each said Payment Bank Host Application having means for processing payment messages, including payments instructions to be carried out in said domestic payments system on behalf of a plurality of account holders (including bank correspondents), and

wherein each said Payment Bank Host Application includes a filter process module for automated processing of said payments instructions based on (i) payments risk parameters and (ii) the accounts of said Users (User accounts) such that payments instructions breaching said payments risk parameters are rejected back to a payments processing queue for later re-evaluation, thereby reducing payments risk, liquidity risk and systemic risk throughout said system.

2. The system of claim 1, wherein each Third Party Host Application, said User Host Application and said Payment Bank Host Application sends payments risk data and generates and receives payments-related notifications, inquiries, messages and reports via their respective host applications.

3. The system of claim 1, wherein said Filter Process Module in each said Payment Bank Host Application is integrated with payments processing such that payments instructions are filtered for compliance using suspend payment instructions and said payments risk parameters.

4. The system of claim 1, wherein each said Third Party Host Application and said User Host Application can request and receive - whether periodically or on-demand - multi-currency reports from said plurality of Payment Bank Host Applications.

5. The system of claim 1, wherein each said Payment Bank Host Application is capable of calculating the Available Balance for counterparty payments using data interchange with existing payments confirmation services and monitoring elapsed time.

6. The system of claim 5, wherein each said Payment Bank Host Application can generate a notification to the Payment Bank and User and/or Third Party in the event that a counterparty fails to make expected payments for a pre-determined period of elapsed time.

7. The system of claim 6, wherein each Third Party or User receiving notification of a counterparty payment failure may instruct Payment Bank to suspend and/or reinstate further payments to said counterparty.

8. The system of claim 6, wherein each said Payment Bank Host Application automatically incorporates a suspension of all further payments to a counterparty on receipt of a notification to do so via implementation as a trigger in said Filter Process Module.

9. The system of claim 1, wherein each Payment Bank and User use digital certification to establish their access authority and usage constraints, and wherein data transmissions over said communication network are encrypted for security purposes.

10. The system of claim 1, wherein said Third Party, User and Payment Bank Host Applications are human-accessible by browser interface and machine-accessible by incorporation and translation of electronic data interchange formats.

11. The system of claim 1, wherein Third Parties and Users can flexibly identify counterparties by means of aggregating identifiers unique to individual corporate or organizational entities, creating thereby synthetic counterparties composed of entities deemed to share correlation in payment risk assessment.

12. The system of claim 1, which further comprises a processor-based Core System being operably connected to said global communications network and supporting a Core System Host Application, wherein said Core System Host Application comprises information storage means for recording various type of information, including identification of said Users, identification of said Third Parties, identification of said Payment Banks, identification of said counterparties, identification of currencies, specification of the Clean Payment Limit (Debit Cap), and Payment Type identification (including alternative payment channels, if any).

13. A method of reducing payments risk, liquidity risk, and systemic risk in a system supporting a plurality of Third Party Host Applications, a plurality of User Host Applications, and a plurality of Payment Bank Host Applications, each said payment Bank Host Application has a Filter Process Module for processing payments instructions, said method comprising the steps:

(a) said Third Parties sending counterparty payments risk data to said Users associated with a plurality of payments-based transactions;

(b) said Users sending counterparty payments risk data on behalf of themselves and said Third Parties to said system, wherein said payments risk data specifies transaction parameters selected from the group consisting of

(i) the User associated with each said payments-based transaction,

(ii) the Third Party (if any) associated with each said payments-based transaction,

(iii) the Payment Bank associated with each said payments-based transaction,

(iv) the intermediary(ies) in the chain of accounts leading to the counterparty or ultimate payment beneficiary,

(v) the counterparty associated with each said payments-based transaction,

(vi) the currency associated with each said payments-based transaction,

(vii) the payment type associated with each said payments-based transaction,

(viii) the Transaction Reference Number unique to each payment transaction, and

(ix) the Clean Payment Limit associated with each said payments-based transaction;

(c) said system analysing the payments risk data associated with each said payments-based transaction and decomposing said payments risk data into files for transfer to said Payment Bank Host Applications making payments on behalf of said Users in a plurality of currencies;

(d) said system transmitting said payments risk data, associated with each said payments-based transaction, to said Payment Bank Host Applications, using application-to-application automated interfaces; and

(e) each said Payment Bank Host Application applying said payments risk data as input parameters to said Filter Process Module for automated evaluation of payments instructions in respect of accounts of said Users (User accounts) such that payments instructions breaching said input parameters to said Filter Process Module are rejected back to a payments processing queue for later re-evaluation in the absence of an override instruction.

14. The method of claim 13, wherein each Third Party, User and Payment Bank sending payments risk data can also generate and receive payments-related notifications, inquiries, messages and reports via their respective host applications.

15. The method of claim 13, wherein said Filter Process Module within each said Payment Bank Host Application cooperates with payments processing with said domestic payment system

operated by said Payment Bank, such that payments instructions are filtered by said Filter Process Module for compliance with suspend instructions, override instructions and payment risk parameters.

16. The method in claim 14, wherein each Third Party and User can request and receive reports from a plurality of said Payment Banks acting on their behalf.

17. The method of claim 13, wherein each said Payment Bank Host Application capable of calculating the Available Balance for counterparty payments through incorporation of data interchange with existing payments confirmation services and monitoring elapsed time.

18. The method of claim 14, wherein each Payment Bank Host Application can generate a notification to the Payment Bank and User and/or Third Party in the event that a counterparty fails to make expected payments for a pre-determined period of elapsed time and detail payments which have failed to pass the Filter Process according to their Transaction Reference Numbers.

19. The method of claim 18, wherein each Third Party or User receiving notification of a counterparty payment failure may instruct Payment Bank suspension of further payments to said counterparty or instruct override of the Filter Process to allow individual identified payments to proceed or allow payments to specified counterparties or intermediaries.

20. The method of claim 17, wherein each Payment Bank Host Application will automatically incorporate a suspension of all further payments to a counterparty on receipt of a notification to do so via implementation as a trigger in the Filter Process Module and incorporate overrides as instructed.

21. The method of claim 13, wherein each Payment Bank and User are subjected to digital certification to establish their access authority and usage constraints, and wherein data transmissions are encrypted for security purposes.

22. The method of claim 13, wherein Third Party, User and Payment Bank host applications are human-accessible by browser interface and machine-accessible by incorporation and translation of electronic data interchange formats.

23. The method of claim 13, wherein Third Parties and Users can flexibly identify counterparties by means of aggregating identifiers unique to individual corporate or organizational entities, creating thereby synthetic counterparties composed of entities deemed to share correlation in payment risk assessment.

24. The method of claim 13, wherein said system further comprises Core System Host Application for recording various type of information, including identification of said Users, identification of said Third Parties, identification of said Payment Banks, identification of said

counterparties, identification of currencies, specification of the Clean Payment Limit (Debit Cap), any override instructions, and Payment Type identification (including alternative payment channels, if any).

57. A computer-implemented method of reducing risk in a payment-based transaction wherein payment is made from an account holder to a Counterparty using a payment bank system operated by a payment bank, the method comprising the steps of:

receiving at least one user-supplied risk parameter associated with the Counterparty;

receiving a first instruction authorizing payment from the account holder to the Counterparty;

storing the first instruction in a payment queue;

during processing of the payment transaction, performing a risk filter routine that determines whether to selectively reject payment authorized by the first instruction based upon the at least one user-supplied risk parameter associated with the Counterparty.

58. The computer-implemented method of claim 57, further comprising the step of: generating the at least one user-supplied risk parameter on a user system and communicating the at least one user-supplied risk parameter to the risk filter routine.

59. The computer-implemented method of claim 57, wherein the risk filter routine includes the steps of:

generating an available balance for the Counterparty based upon the at least one user-supplied risk parameter, payments made by the account holder, and payments received by the account holder;

reading the first instruction from the payment queue of the payment bank system; and

determining whether to selectively reject payment authorized by the first instruction based upon the available balance.

60. The computer-implemented method of claim 59, wherein payment authorized by the first instruction is rejected in the event that the amount of payment authorized by the first instruction exceeds the available balance.

61. The computer-implemented method of claim 59, wherein the first instruction is returned to the payment queue for later re-evaluation in the event that the amount of payment authorized by the first instruction exceeds the available balance.

62. The computer-implemented method of claim 59, wherein the available balance is computed over a given time period based upon payments made by the account holder in the given time period and payments received by the account holder in the given time period.

63. The computer-implemented method of claim 62, further comprising the steps of:

receiving user-supplied updates to the at least one user-supplied risk parameter; and

updating the available balance to reflect such user-supplied updates.

64. The computer-implemented method of claim 63, further comprising the steps of: generating the user-supplied updates on a user system and communicating the user-supplied updates to the risk filter routine.

65. The computer-implemented method of claim 62, further comprising the steps of:

receiving updates to payments made by the account holder in the given time period; and

receiving updates to payments received by the account holder in the given time period; and

updating the available balance to reflect such updates.

66. The computer-implemented method of claim 65, wherein updates to payments made by the account holder and updates to payments received by the account holder are received through data interchange with existing payments confirmation services.

67. The computer-implemented method of claim 62, further comprising the step of receiving user-supplied updates to the at least one user-supplied risk parameter for use in the risk filter routine.

68. The computer-implemented method of claim 67, further comprising the steps of: generating the user-supplied updates on a user system and communicating the user-supplied updates to the risk filter routine.

69. The computer-implemented method of claim 57, wherein the risk routine is executed by a module integrated into the payment bank system.

70. The computer-implemented method of claim 57, wherein the risk filter routine is executed by a module that communicates to the payment bank system via an application-to application interface which translates data formats between the module and the payment bank system.

71. The computer-implemented method of claim 69, wherein the at least one user-supplied risk parameter is generated on a user system and communicated to a central server, which stores the at least one user-supplied risk parameter in a data server and forwards the at least one user-supplied risk parameter to the module integrated into the payment bank system that executes the risk filter routine.

72. The computer-implemented method of claim 57, wherein the at least one user-supplied risk parameter comprises a clean payment limit.

73. The computer-implemented method of claim 57, wherein the at least one user-supplied risk parameter is associated with each payment-based transaction wherein payment is made from the account holder to the Counterparty.

74. The computer-implemented method of claim 73, wherein the at least one user-supplied risk parameter is selected from the group consisting of:

(i) currency associated with each payment-based transaction,

(ii) payment type associated with each payment-based transaction, and

(iii) a Clean Payment Limit associated with each payment-based transaction.

75. The computer-implemented method of claim 73, wherein the at least one user-supplied risk parameter is associated with a first identifier that identifies the account holder and a second identifier that identifies the Counterparty on the payment transaction.

76. The computer-implemented method of claim 75, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

77. The computer-implemented method of claim 76, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party.

78. The computer-implemented method of claim 77, wherein said third party executes a third party host application that generates the at least one user-supplied risk parameter and communicates the at least one user-supplied risk parameter and associated information to a user system, which forwards the at least one user-supplied information to the risk filter routine.

79. The computer-implemented method of claim 78, wherein only the user system can forward the at least one user-supplied risk parameter communicated by the third party host application to the risk filter routine.

80. The computer-implemented method of claim 75, wherein the first and second identifiers are Bank Identifier Codes or an aggregation of such codes.

81. The computer-implemented method of claim 75, wherein the Counterparty comprises a beneficiary of the payment-based transaction.

82. The computer-implemented method of claim 57, wherein said risk filter routine cooperates with other payment processing operated by said payment bank to determine whether to selectively reject payment authorized by the first instruction.

83. The computer-implemented method of claim 57, wherein the risk filter routine cooperates with a domestic payment system operated by said payment bank, such that the first instruction is filtered by said risk filter routine for compliance with a risk profile generated from the at least one user-supplied risk parameter.

84. The computer-implemented method of claim 57, further comprising the step of : for each given first instruction, when processing by the risk filter routine rejects payment authorized by the given first instruction, adding the given first instruction to a cache of first instructions.

85. The computer-implemented method of claim 57, further comprising the step of communicating notification of rejection or success of at least one payment authorized by the first instructions stored in a cache.

86. The computer-implemented method of claim 85, wherein said notification is communicated via messaging services operably coupling the user system, a central system, and the payment bank system.

87. The computer-implemented method of claim 86, wherein a third party application is operably coupled to the payment bank system, and wherein said notification is forwarded to said third party application by said payment bank system.

88. The computer-implemented method of claim 85, wherein said notification is generated in the event that the Counterparty fails to make expected payments for a pre-determined period of elapsed time.

89. The computer-implemented method of claim 57, further comprising the steps of:

receiving a user-supplied second instruction that identifies an account holder and Counterparty; and

in response to receipt of the user-supplied second instruction, suspending all payments from the account holder to the Counterparty as identified by the second instruction.

90. The computer-implemented method of claim 89, wherein the user-supplied second instruction is generated on a user system and communicated to a central server, which stores the user-supplied second instruction in a data server and forwards the user-supplied second instruction to a module integrated into the payment bank system that executes the risk filter routine.

91. The computer-implemented method of claim 90, wherein a third party executes a third party host application that generates the user-supplied second instruction and communicates the user-supplied second instruction to a user system, which forwards the user-supplied second instruction to the module integrated into the payment bank system via the central server.

92. The computer-implemented method of claim 89, further comprising the step of: communicating notification confirming receipt and implementation of the user-supplied second instruction to the payment bank, core server, user and third party, if any.

93. The computer-implemented method of any of claim 89, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

94. The computer-implemented method of claim 93, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party as payment intermediary.

95. The computer-implemented method of claim 94, wherein said third party executes a third party host application that generates user-supplied instructions and communicates the user-supplied instructions to a user system, which forwards the at least one user-supplied instruction to the risk filter routine.

96. The computer-implemented method of any of claim 89, wherein the Counterparty comprises a payment beneficiary of the payment-based transaction.

97. The computer-implemented method of claim 57, further comprising the step of: using digital certification to establish access authority and usage constraints of the risk filter routine.

98. The computer-implemented method of claim 57, wherein data transmissions are encrypted for security purposes.

99. The computer-implemented method of claim 57, wherein users and the payment bank can also generate and receive payments-related notifications, inquiries, messages and reports.

100. The computer-implemented method of claim 57, wherein users can request and receive multi-currency reports from a plurality of Payment Banks acting on their behalf.

101. The computer-implemented method of claim 57, wherein human-accessibility is provided by browser interfaces and data-accessibility is provided by electronic data interchange formats.

102. The computer-implemented method of claim 57, wherein said account holder and Counterparty comprise multiple entities that are deemed to share correlation in payment risk assessment, wherein the multiple entities are identified by an aggregate identifier.

103. The computer-implemented method of claim 57, further comprising the steps of: recording various type of information, including identification of Users, identification of Third Parties, identification of Payment Banks, identification of Counterparties, identification of Currencies, specification of the Clean Payment Limit, and Payment Type identification.

104. The computer-implemented method of claim 57, wherein selective rejection of payment authorized by the first instruction reduces payment risk arising from default by the Counterparty and any liquidity risk and system risk arising therefrom in like amount.

105. A system for reducing risk in payment-based transactions comprising:

a payment bank subsystem, operated by a payment bank, that processes a payment-based transaction wherein payment is made from an account holder to a Counterparty, wherein the payment bank subsystem includes a queue storing a first instruction authorizing payment from the account holder to the Counterparty during processing of the transaction; and

a module, integrated with the payment bank subsystem, that stores at least one user-supplied risk parameter associated with the account holder, and includes a risk filter routine that operates during processing of the transaction to determine whether to selectively reject payment authorized by the first instruction stored in the queue based upon the at least one user-supplied risk parameter associated with the Counterparty.

106. The system of claim 105, wherein the risk filter routine:

generates an available balance for the Counterparty based upon the at least one user-supplied risk parameter, payments made by the account holder, and payments received by the account holder;

accesses a first instruction stored in the queue; and

determines whether to selectively reject payment authorized by the first instruction based upon the available balance.

107. The system of claim 106, wherein the risk filter routine rejects payment authorized by the first instruction in the event that the amount of payment authorized by the first instruction exceeds the available balance.

108. The system of claim 106, wherein the risk filter routine returns the first instruction to the payment queue for later re-evaluation.

109. The system of claim 106, wherein the risk filter routine computes the available balance over a given time period based upon payments made by the account holder in the given time period and payments received by the account holder in the given time period.

110. The system of claim 109, wherein the risk filter routine receives user-supplied updates to the at least one user-supplied risk parameter, and updates the available balance to reflect such user-supplied updates.

111. The system of claim 109, wherein the risk filter routine receives updates to payments made by the account holder in the given time period and updates to payments received by the

account holder in the given time period, and re-computes the available balance to reflect such updates.

112. The system of claim 111, further comprising a payment confirmation service, and wherein the risk filter routine receives updates to payments made by the account holder and updates to payments received by the account holder through data interchange with the payments confirmation service.

113. The system of claim 105, wherein the module communicates to the payment bank subsystem via an application-to application interface which translates data formats between the module and the payment bank subsystem.

114. The system of claim 105, wherein the at least one user-supplied risk parameter comprises a clean payment limit.

115. The system of claim 105, wherein the at least one user-supplied risk parameter is associated with each payment-based transaction wherein payment is made from the account holder to a Counterparty.

116. The system of claim 105, wherein the at least one user-supplied risk parameter is selected from the group consisting of:

(i) currency associated with each payment-based transaction,

(ii) payment type associated with each payment-based transaction, and

(iii) a Clean Payment Limit associated with each payment-based transaction;

117. The system of claim 115, wherein the at least one user-supplied risk parameter is associated with a first identifier that identifies the account holder and a second identifier that identifies the Counterparty as payment beneficiary or intermediary on the payment transaction.

118. The system of claim 117, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

119. The system of claim 118, wherein the system includes a user subsystem executing a user host application that generates the at least one user-supplied risk parameter on a user subsystem and communicates the at least one user-supplied risk parameter to the module for use in the risk filter routine.

120. The system of claim 119, wherein the user subsystem generates user-supplied updates to the at least one user-supplied risk parameter and communicates the user-supplied updates to the module for use in the risk filter routine.

121. The system of claim 118, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party.

122. The system of claim 121, further comprising a third party host application that enables the third party to generate the at least one user-supplied risk parameter and communicate the at least one user-supplied risk parameter and associated information to a user subsystem, which forwards the at least one user-supplied information to the module for use in the risk filter routine.

123. The system of claim 122, wherein the third party host application enables the third party to generate updates to the least one user-supplied risk parameter and communicate the updates and associated information to a user subsystem, which forwards the updates and associated information to the module for use in the risk filter routine.

124. The system of claim 122, wherein only the user subsystem can forward the at least one user-supplied risk parameter communicated by the third party host application to the module for use in the risk filter routine.

125. The system of any of claims 118 to 124, wherein user-supplied risk parameter and updates thereto are communicated from the user subsystem to a central server, which stores the at least one user-supplied risk parameter and updates thereto in a data server and forwards the user-supplied risk parameter and updates thereto to the module for use in the risk filter routine.

126. The system of claim 117, wherein the first and second identifiers are Bank Identifier Codes.

127. The system of claim 117, wherein the Counterparty comprises a payment beneficiary of the payment-based transaction.

128. The system of claim 105, wherein said risk filter routine cooperates with other payment processing operated by said payment bank to determine whether to selectively reject payment authorized by the first instruction.

129. The system of claim 105, wherein the risk filter routine cooperates with a domestic payment system operated by said payment bank, such that the first instruction is filtered by said risk filter routine for compliance with a risk profile generated from the at least one user-supplied risk parameter.

130. The system of claim 105, wherein the risk filter routine, when processing a given first instruction results in a determination to selectively reject payment authorized by the given first instruction, and, whether selectively rejected or not, adds the given first instruction to a cache of first instructions.

131. The system of claim 130, wherein the risk filter routine triggers communication of a notification of rejection of at least one payment authorized by the first instructions stored in the cache to a user subsystem of the Payment Bank.

132. The system of claim 131, wherein said notification is communicated via messaging services operably coupling the user subsystem, a central subsystem, and the payment bank subsystem.

133. The system of claim 132, further comprising a third party application operably coupled to the user subsystem, wherein said notification is forwarded to said third party application by said user subsystem.

134. The system of claim 131, wherein said notification is generated in the event that the Counterparty fails to make expected payments for a pre-determined period of elapsed time.

135. The system of claim 105, wherein the risk filter routine:

receives a user-supplied second instruction that identifies an account holder and Counterparty; and

in response to receipt of the user-supplied second instruction, suspends all payments from the account holder to the Counterparty as identified by the second instruction.

136. The system of claim 135, wherein the user-supplied second instruction is generated on a user subsystem and communicated to a central server, which stores the user-supplied second instruction in a data server and forwards the user-supplied second instruction to a module integrated into the payment bank subsystem that executes the risk filter routine.

137. The system of claim 136, wherein a third party executes a third party host application that generates the user-supplied second instruction and communicates the user-supplied second instruction to a user subsystem, which forwards the user-supplied second instruction to the module integrated into the payment bank subsystem via the central server.

138. The system of claim 136, wherein the risk filter routine triggers communication of notification confirming receipt of the user-supplied second instruction to the payment bank subsystem, core server, user subsystem and third party subsystem, if any.

139. The computer-implemented method of any of claim 135, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

140. The system of claim 139, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party.

141. The system of claim 140, wherein said third party executes a third party host application that generates user-supplied instructions and communicates the user-supplied instructions to a user subsystem, which forwards the at least one user-supplied information to the risk filter routine.

142. The system of any of claim 135, wherein the Counterparty comprises a beneficiary of the payment-based transaction.

143. The system of claim 105, wherein digital certification is used to establish access authority and usage constraints of the risk filter routine.

144. The system of claim 105, wherein data transmissions are encrypted for security purposes.

145. The system of claim 105, wherein users and the payment bank can also generate and receive payments-related notifications, inquiries, messages and reports.

146. The system of claim 105, wherein users can request and receive multi-currency reports from a plurality of Payment Banks acting on their behalf.

147. The system of claim 105, wherein human-accessibility is provided by browser interfaces and data-accessibility is provided by electronic data interchange formats.

148. The system of claim 105, wherein said account holder or Counterparty may comprise multiple entities that are deemed to share correlation in payment risk assessment, wherein the multiple entities are identified by an aggregate identifier.

149. The system of claim 105, further comprising a central core that records various type of information, including identification of Users, identification of Third Parties, identification of Payment Banks, identification of Counterparties, identification of Currencies, specification of the Clean Payment Limit, and Payment Type identification.

150. The system of claim 105, wherein selective rejection of payment authorized by the first instruction minimizes payment risk arising from default by the Counterparty and any liquidity risk and system risk arising therefrom.

151. The system of claim 144, wherein the data transmissions occur over a VPN that uses the Internet and other internet protocol telecommunication networks.

152. The system of claim 105, wherein the risk filter routine controls the flow of payment messages from the payment queue to a domestic payment system for clearance.